(d)[(f)] receiving [from the service provider] said selected event **from the service provider**, said selected event being scrambled using said **descrambling** [event] key; and

(e)[(g)]descrambling said selected event using said **descrambling** [event] key [to provide a descrambled event].

2. (Amended) The method of Claim 1 wherein the steps of decrypting said message, receiving said selected event, and descrambling said selected event are performed in a smart card coupled to the device, said **message being encrypted using a public key** [second private and public keys being] associated with said smart card and **said step of decrypting uses a private key associated with and** [said second private key being] stored in said smart card.

3. (Amended) The method of Claim 2 wherein said message further comprises event information, said event information being decrypted using said [second] private key.

4. (Amended) The method of Claim 3 further comprising the step of storing said event information, wherein said step of storing said event information is performed in said [removable] smart card.

6. (Amended) The method of Claim 5 **further comprising** [wherein the step of] authenticating **said list of events** [comprises decrypting said digital signature in said device] to verify the origin of said message.

7. (Amended) The method of Claim 6 wherein **each message further comprises a digital signature created using a second private key and the step of authenticating comprises decrypting said digital signature using a** [said first] **second** public key **that** is stored in said device

10. (Amended) The method of Claim **7** [1] wherein said digital signature, said **second** [first] public key and said **second** [first] private key are issued by an independent certificate authority and are associated with said list provider.

15. (Amended) A method for managing access between a device having a smart card coupled thereto and a service provider, said device performing the steps of:

2

(a)   receiving an electronic program guide from a guide provider, said guide having [a digitally signed message corresponding to each event in said guide, each of said digitally signed messages comprise] a message **and a digital signature associated with each event in said guide, said message being** encrypted using a public key of the smart card and **said** [a] digital signature **being** created using a private key of said guide provider;

(b)   selecting an event from said guide;

(c)   receiving said [digitally signed] **encrypted** message **and said digital signature** corresponding to the selected event;

(d)   authenticating said guide provider by decrypting said digital signature using a public key of said guide provider, said guide public key being stored in said device;

(e)   passing said message to **said** [a] smart card [coupled to the device];

(f)   decrypting, **in said smart card,** said message using a private key of **said** [the] smart card to obtain event information and a symmetric key, said smart card private key being stored within **said** [the] smart card;

(g)   storing said event information in **said** [the] smart card and updating account information based on said event information;

(h)   receiving from the service provider said selected event, said selected event being scrambled using said symmetric key; and

(i)   descrambling, in said smart card, said selected event using said symmetric key to generate a descrambled event.

18.   (Amended)   A method for managing access between a device having a smart card coupled thereto and a service provider, said device performing the steps of:

(a)   receiving an electronic program guide **from a guide provider**, said guide having a digital certificate and a separate message corresponding to each event in said guide, each of said digital certificates being encrypted using a first private key of said guide, said separate message being encrypted using a public key of the smart card and having an associated digital signature created using a second private key of said guide;

(b)   selecting an event from said guide;

(c)   receiving said digital certificate, said message and said digital signature corresponding to the selected event;

(d)   authenticating said guide provider by decrypting said digital certificate using a first public key of said guide to obtain a second public key of said guide, and